2

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年12月6日 (06.12.2001)

PCT

(10) 国際公開番号
WO 01/93139 A1

(51) 国際特許分類[7]: G06F 17/60

(21) 国際出願番号: PCT/JP01/04538

(22) 国際出願日: 2001年5月30日 (30.05.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-163676 2000年5月31日 (31.05.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目11番1号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 木下眞希 (KINOSHITA, Masaki) [JP/JP]; 〒124-0004 東京都葛飾区東堀切一丁目16-10 Tokyo (JP). 山下哲也 (YAMASHITA, Tetsuya) [JP/JP]; 〒158-0091 東京都世田谷区中町二丁目23-10-202 Tokyo (JP).

(74) 代理人: 川崎研二(KAWASAKI, Kenji); 〒103-0027 東京都中央区日本橋一丁目2番10号 東洋ビルディング7階 朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, CN, KR, US.

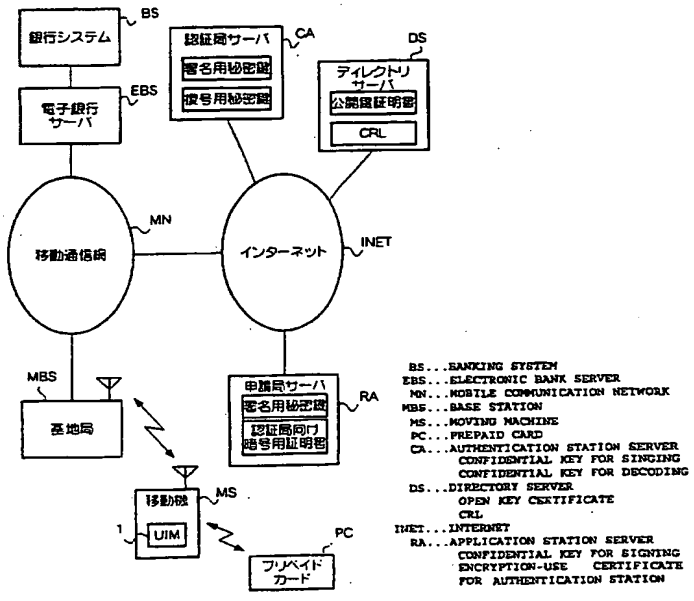
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: ELECTRONIC VALUE SYSTEM

(54) 発明の名称: 電子バリューシステム



(57) Abstract: An efficient tracking of amount of money in an electronic money information system is implemented. A moving machine, which is typically a portable phone mounted thereon with a UIM (User Identity Module) carrying electronic values, transfers values with an electronic bank server, other moving machines and apparatuses incorporating moving machines. The electronic bank server keeps track of a value deposited in an electronic value account and a value balance downloaded to the UIM, and updates these values on receiving a signed log for value transferred transactions. The log is transmitted periodically or as needed by one or both of the moving machines at transaction-related parties.

[続葉有]

WO 01/00000 A1

明細書

電子バリューシステム

技術分野

本発明は、電子バリューを用いて電子商取引を行うための電子バリューシステムに関する。

背景技術

電子的な金銭情報（以下、電子バリューと呼ぶ）を用いて、キャッシュレスショッピングを行うためのシステムが各種提案されている。

ところが、電子バリューは単なるデータにすぎないため、データそのものが改ざんされたり、第三者が電子バリューの所有者になりすますなどの不正が発生する虞があり、これを防止するためのセキュリティの確保が課題となっている。

一方、セキュリティ確保のためのシステムを動作させるということは、そのための処理が増大することをも意味しており、システム全体の処理効率を劣化させる要因となる。

発明の開示

本発明は、このような背景に鑑みてなされたものであり、セキュリティを確保するとともに、処理効率を向上させる電子バリューシステム、通信端末及びサーバを提供することを目的とする。

かかる目的を達成するため、この発明は、各々、電子バリューを格納するメモリと、外部ノードとの間で電子バリューを送受信する通信手段とを有し、ユーザの電子財布としての役割を果たす複数の通信端末と、ネットワーク上のサーバに設けられ、複数のユーザのそれぞれに割り当てられた電子口座毎に、電子バリュ

好ましい態様において、前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する量の前記取引ログを蓄積すると、外部ノードと電子バリューの送受信を行わない。

また、別の好ましい態様によると、前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する量の前記取引ログを蓄積すると、それ以後の取引時においては取引日時の古い順から前記取引ログを消去する。

さらに別の好ましい態様では、前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、前記取引ログ通知手段は、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方において前記ログ蓄積手段による記憶容量に相当する量の前記取引ログを蓄積すると、当該取引ログを前記財布残金管理手段に送信する。

以上説明した電子バリューシステムの諸態様において、例えば、前記通信端末は、移動通信網に収容される移動通信端末であり、前記ネットワークは、前記移動通信網であり、前記第１の通信端末及び第２の通信端末は、無線により通信を行ってもよい。また、前記通信端末のメモリは、例えば当該通信端末に装着して使用されるＩＣカードであってもよい。また、前記通信端末は、前記電子バリューを外部に送信する際には、その送信日時を当該電子バリューに付加して送信してもよい。また、前記通信端末は、外部と前記電子バリューを送受信する際に、当該電子バリューに対し鍵を用いて電子認証及び暗号・復号の処理を行うセキュリティ手段と、前記鍵を定期的に更新する更新手段とを備えていてもよい。

また、この発明は、第１の通信端末及び第２の通信端末の間で、電子的な金銭情報である電子バリューを送受信する電子バリューシステムであって、前記第１の通信端末は、前記電子バリューと、前記電子バリューを発行した発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納

と当該識別情報に対し前記発行主体によって施された電子署名を取得する取得手段と、前記取得した電子署名を検証し、前記第２の通信端末のメモリ内の電子バリューは前記発行主体により発行されたことを確認することによって、前記第２の通信端末の正当性を判断する判断手段とをさらに備える。

また、電子バリューシステムにおいて、前記第１の通信端末及び前記第２の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、前記第１の通信端末又は前記第２の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、自身が記憶している電子バリューの残高情報を管理している外部ノードに対し、前記蓄積した取引ログを送信するようにしてもよい。

また、前記第１の通信端末及び前記第２の通信端末は、無線により電子バリューの送受信を行ってもよい。前記第１の通信端末又は前記第２の通信端末の少なくともいずれか一方は、移動通信網に収容される移動通信端末であってもよい。また、前記第２の通信端末は、例えば商品を販売する自動販売機に内蔵されていてもよい。前記通信端末は、前記電子バリューを外部に送信する際には、その送信日時を当該電子バリューに付加して送信してもよい。また、前記通信端末は、外部と前記電子バリューを送受信する際に、当該電子バリューに対し鍵を用いて電子認証及び暗号・復号の処理を行うセキュリティ手段と、前記鍵を定期的に更新する更新手段とを備えていてもよい。

また、この発明は、電子的な金銭情報である電子バリュー及び自己の識別情報を格納するメモリと、外部ノードとの間で前記電子バリューの送受信を行う通信手段と、前記メモリに格納されている自己の識別情報を前記外部ノードに与える一方、前記外部ノードから当該外部ノードの識別情報を取得する識別情報交換手段と、前記外部ノードとの間で送受信された前記電子バリューの額と、前記自己の識別情報及び前記外部ノードの識別情報とを取引ログとして蓄積するログ蓄積手段とを備えることを特徴とする通信端末を提供する。

好ましい態様において、通信端末は、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、前記外部ノードとの間で前記電子バリューの送

時を前記電子バリューに付加して送信してもよい。前記通信手段は、無線により前記外部ノードとの間で前記電子バリューの送受信を行ってもよい。前記通信端末は、例えば移動通信網に収容される移動通信端末であり、前記メモリは、当該通信端末に装着して使用されるＩＣカードである。

また、この発明は、電子的な金銭情報である電子バリューを記憶するサーバであって、ユーザに割り当てられた電子口座毎に前記電子バリューを蓄積する電子口座保持手段と、前記電子バリューを格納するメモリと、外部ノードとの間で前記電子バリューを送受信する通信手段とを有した通信端末に対し、前記電子口座保持手段によって蓄積されている電子バリューを前記ネットワークを介して移す移行手段と、前記通信端末のメモリに格納される電子バリューの残高情報を記憶する財布残金記憶手段とを備え、前記通信端末における前記電子バリューを用いた取引の内容を示す取引ログを、前記通信端末から前記ネットワークを介して取得するログ取得手段と、前記取得した取引ログに基づいて、前記財布残金記憶手段により記憶されている前記電子バリューの残高情報を更新する財布残金更新手段とを備えることを特徴としたサーバを提供する。

好ましい態様において、前記サーバは、前記ダウンロードされる電子バリュー情報に対し、自身が記憶する鍵により電子認証を施す電子認証手段を備える。

図面の簡単な説明

図１は、本発明の実施形態に係るシステム全体の構成を示すブロック図である。

図２は、同実施形態における電子銀行サーバの構成を示すブロック図である。

図３は、同実施形態における電子銀行サーバ内のデータベースの記憶内容を説明する図である。

図４は、同実施形態における電子銀行サーバ内のデータベースの記憶内容を説明する図である。

図５は、同実施形態における電子銀行サーバ内のデータベースの記憶内容を説明する図である。

図１は、実施形態にかかわるシステム全体の構成を示すブロック図である。同図に示すように、このシステムは、移動機ＭＳ、移動通信網ＭＮ、プリペイドカードＰＣ、電子銀行サーバＥＢＳ、銀行システムＢＳ、インターネットＩＮＥＴ、申請局サーバＲＡ、認証局サーバＣＡ、ディレクトリサーバＤＳから構成される。

プリペイドカードＰＣは、電子バリューに関する電子バリュー情報を予め格納した非接触ＩＣカードである。このプリペイドカードＰＣは、格納している電子バリュー情報を無線により外部ノードに送信する機能を備えており、ユーザの電子財布として機能するものである。この実施形態では、例えばＩｒＤＡ（Infrared Data Association）等の赤外線を用いる。

移動機ＭＳは、例えば携帯電話機であり、移動通信網ＭＮを介して音声通信やデータ通信を行う。この移動機ＭＳは、電子バリューに関する電子バリュー情報の記憶及び入出力を司るＩＣカードを内蔵する。以下、このＩＣカードをＵＩＭ（User Identity Module）１と呼ぶ。ユーザは、このＵＩＭ１を移動機ＭＳに装着することにより、この移動機ＭＳを電子財布として動作させることが可能となる。

具体的には、移動機ＭＳは、ＵＩＭ１内の電子バリュー情報を読み出し、これを外部ノードとやり取りすることにより、各種の商取引を実現する。この電子バリューをやり取りする形態としては、移動通信網ＭＮを介して電子銀行サーバＥＢＳあるいは他の移動機ＭＳと電子バリュー情報を送受信する場合と、プリペイドカードＰＣから赤外線によって送信された電子バリュー情報を送受信する場合とがある。

移動通信網ＭＮは、基地局ＭＢＳや図示せぬ交換局からなり、移動機ＭＳに対し音声通信サービスやデータ通信サービスを提供する。この移動通信網ＭＮは、図示せぬゲートウェイ装置を介してインターネットＩＮＥＴに接続されている。

電子銀行サーバＥＢＳは、移動通信網ＭＮに接続されるほか、図示せぬ銀行内に設置された銀行システムＢＳに専用線により接続されている。この電子銀行サーバＥＢＳには、各ユーザに割り当てられた仮想的な銀行口座（以下、電子口座と呼ぶ）が開設されている。電子銀行サーバＥＢＳは、電子口座を特定するため

移動機ＭＳや電子銀行サーバＥＢＳの通信相手となるノードは、ディレクトリサーバＤＳから公開鍵証明書を取得して電子署名を検証することにより、第三者が当該通信相手になりすましていないかを確認することができる。

申請局サーバＲＡは、インターネットＩＮＥＴ上に設けられたサーバであり、ユーザによる電子口座の開設申請を受け付け、電子銀行サーバＥＢＳ、認証局ＣＡ及びディレクトリサーバＤＳと連携して電子口座の開設に関する処理を実行する。

この申請局サーバＲＡは、署名用秘密鍵と、認証局向け暗号用証明書とを記憶している。署名用秘密鍵とは、申請局サーバＲＡが外部ノードに送信すべきデータに対し電子署名を施すための鍵であり、これにより、第３者が申請局サーバＲＡになりすますことを防止する。また、認証局向け暗号用証明書とは、認証局サーバＣＡに送信すべきデータを暗号化するための公開鍵の証明書である。この認証局向け暗号用証明書による暗号文は、認証局サーバＣＡが所有している復号用秘密鍵によって復号される。これにより、認証局サーバＣＡに送信するデータを第３者が盗聴することを防止することができる。

（２）電子銀行サーバＥＢＳの構成

次に、図２に示すブロック図を参照しながら、電子銀行サーバＥＢＳの構成について説明する。

同図に示すように、電子銀行サーバＥＢＳは、通信部１１、制御部１２、データベース１３、及びこれらを相互に接続するバス１４から構成される。

通信部１１は、インターネットＩＮＥＴとの接続インタフェース（図示略）や通信制御回路（図示略）からなる。この通信部３１は、移動通信網ＭＮ及びインターネットＩＮＥＴを介して認証局サーバＣＡ、ディレクトリサーバＤＳとデータ通信を行うほか、移動通信網ＭＮを介して移動機ＭＳとデータ通信を行う。

制御部１２は、図示せぬＣＰＵ（Central Processing Unit）、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）から構成され、この電子銀行サーバＥＢＳ全体を制御する。

データベース１３には、図３に示すように、「署名用秘密鍵」、「復号用秘密

とアクセスした時点における、電子口座内の電子バリューの残高である。

「ＵＩＭの電子バリュー額」は、移動機ＭＳが最後に電子銀行サーバＥＢＳとアクセスした時点における、ＵＩＭ１内の電子バリューの残高である。

「電子バリュー更新時タイムスタンプ」は、「ＵＩＭの電子バリュー額」が更新された日時を示す情報であり、電子銀行サーバＥＢＳによって発行される。このタイムスタンプを用いることにより、後述するようにして電子バリューの不正再送を発見することができる。

「電子口座のカレント電子バリュー額」は、電子口座内の現在の電子バリューの残高である。

「ＵＩＭのカレント電子バリュー額」は、ＵＩＭ１に反映すべき電子バリューの残高である。後述するように、移動機ＭＳどうしで電子銀行サーバＥＢＳを介さずに電子バリューをやり取りする場合に、そのやり取りの後にこの移動機のうちいずれか一方から電子銀行サーバＥＢＳに取引ログの通知がある。この通知があると、電子銀行サーバＥＢＳでは、双方の移動機ＭＳに格納されるべき電子バリュー額が計算される。この際の、電子銀行サーバＥＢＳと通信を行っていない側の移動機ＭＳ内のＵＩＭ１に反映すべき電子バリュー額が、このＵＩＭのカレント電子バリュー額に相当する。

「カレント電子バリュー額更新時タイムスタンプ」は、電子口座のカレント電子バリュー額及びＵＩＭのカレント電子バリュー額が更新された日時を証明するものである。このタイムスタンプを用いることにより、後述するようにして電子バリューの不正な再送を発見することができる。

「電子バリュー更新履歴」は、移動機ＭＳが最後に電子銀行サーバＥＢＳとアクセスした時点から現在に至るまでの「ＵＩＭの電子バリュー額」の更新履歴である。

次に、図５を参照しながら、プリペイドカードＰＣに格納される電子バリュー情報を管理するための電子バリュー管理情報について説明する。同図に示す電子バリュー管理情報が、図４に示す電子バリュー管理情報と異なる点は、ＵＩＭ１に代えてプリペイドカードＰＣを電子財布の対象としているところと、「電子口

用証明書」、「ユーザＩＤ」及び「電子バリュー情報」が記憶されている。

「署名用秘密鍵」は、移動機ＭＳが外部ノードに対して送信するデータに電子署名を施すための秘密鍵である。このように、外部ノードに対して送信するデータに電子署名を施すことにより、第３者が移動機ＭＳのユーザになりすますことが防止される。

「復号用秘密鍵」は、移動機ＭＳが受信した暗号文を復号するための秘密鍵である。このように、移動機ＭＳに対しては暗号文が送信されてくるため、第３者の盗聴が防止される。

「電子銀行署名検証用証明書」は、電子銀行サーバＥＢＳが署名した電子署名を検証するための公開鍵の証明書である。即ち、電子銀行サーバＥＢＳは、移動機ＭＳ宛のデータに電子署名を施すため、第３者が電子銀行サーバＥＢＳになりすますことが防止される。

「電子銀行向け暗号用証明書」は、電子銀行サーバＥＢＳに対して送信するデータを暗号化するための公開鍵の証明書である。即ち、移動機ＭＳから電子銀行サーバＥＢＳに送信されるデータは暗号化されるため、第３者の盗聴が防止される。

「認証局署名検証用証明書」は、認証局サーバＣＡが各種証明書に施した電子署名を検証するための公開鍵の証明書である。これによって、認証局サーバＣＡが発行した証明書の信頼性が確保される。

「ユーザＩＤ」は、移動機ＭＳのユーザを特定するための識別情報である。

次に、電子バリュー情報は、図８に示すように、「電子銀行ＩＤ」、「電子財布種別」、「電子口座番号」、「電子銀行署名ＳＧＮ１」、「電子口座の電子バリュー額」、「ＵＩＭの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ２」、「カレント電子バリュー額」、「電子バリュー更新履歴」からなる。

「電子銀行ＩＤ」は、既述のとおりである。

「電子財布種別」は、電子バリュー情報を格納する電子財布が、ＵＩＭ１であるかプリペイドカードＰＣであるかということを示す情報である。

リペイドカードＩＤ」が更新履歴として登録される。

「取引金額」は、取引される電子バリューの額であり、「取引相手電子署名」は、上記「受取側電子口座番号」、「支払側電子口座番号」、「支払側プリペイドカードＩＤ」、「取引金額」に改ざんがないことを保証するために取引相手の移動機ＭＳが施した電子署名である。

移動機ＭＳは、取引後において、上述したような「電子バリュー更新履歴」を電子銀行サーバＥＢＳに送信するようになっている。

（３）プリペイドカードＰＣの構成

次に、プリペイドカードＰＣに記憶されるデータについて説明する。

図１０は、プリペイドカードＰＣに記憶されるデータを示す図である、同図に示すように、プリペイドカードＰＣには、「電子銀行署名検証用証明書」、「電子銀行向け暗号用証明書」、「認証局署名検証用証明書」、及び「電子バリュー情報」が記憶されている。

「電子銀行署名検証用証明書」、「電子銀行向け暗号用証明書」及び「認証局署名検証用証明書」は、ＵＩＭ１が記憶しているものと共通する情報であるので説明を省略する。

また、プリペイドカードＰＣには、ＵＩＭ１が記憶している「署名用秘密鍵」及び「復号用秘密鍵」は記憶されていない。これは、移動機ＭＳの場合とは異なり、プリペイドカードは譲渡可能であることから、プリペイドカードＰＣを所持しているユーザが正当な所有者であると認められるので、第三者によるなりすましを防止するための電子署名を行う必要もないし、プリペイドカードＰＣに送られてくる電子バリュー情報のデータが暗号化されて送られてくることもないからである。

次に、図１１を参照しながら、プリペイドカードＰＣ内の電子バリュー情報について詳細に説明する。同図に示すように、電子バリュー情報は、「電子銀行ＩＤ」、「電子財布種別」、「プリペイドカードＩＤ」、「電子銀行署名ＳＧＮ３」、「プリペイドカードの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ４」、「カレント電子バリュー額」、「電子バリュ

ＳＺ２）。この時点で、「電子口座番号」が発行され、この電子口座の有効期限が設定される。

次いで、電子銀行サーバＥＢＳは、「電子口座番号」及び電子口座の有効期限を申請局サーバＲＡに送信する（ステップＳＺ３）。

申請局サーバＲＡは、「電子口座番号」及び電子口座の有効期限を受信すると、これに応じて、ユーザに対応した鍵対（即ち、秘密鍵と公開鍵のペア）を生成する。この鍵対には、移動機ＭＳから電子銀行サーバＥＢＳに送信すべきデータの電子署名とその検証のための鍵対と、電子銀行サーバＥＢＳから移動機ＭＳへ送信すべきデータの暗号・復号のための鍵対との２種類のものがある。この鍵対の有効期限は、電子口座番号の有効期限と同一である。

そして、申請局サーバＲＡは、「電子口座番号」とともに、作成した鍵対のうちの電子署名を検証するための公開鍵及び暗号化を行うための公開鍵を、認証局サーバＣＡに送付し、これらの鍵に対する公開鍵証明書を発行することを依頼する（ステップＳＺ４）。

これに応じて、認証局サーバＣＡは、電子署名検証用及び暗号用の公開鍵証明書を発行し、これらを「電子口座番号」と関連付けてディレクトリサーバＤＳに登録する（ステップＳＺ５）。

一方、電子銀行サーバＥＢＳは、ディレクトリサーバＤＳにアクセスし「電子口座番号」を手がかりに検索をすることによって、電子署名検証用及び暗号用の公開鍵証明書が登録されたことを確認する（ステップＳＺ６）。この時点で電子銀行サーバＥＢＳと移動機ＭＳとの間でセキュリティが確保された通信を行う準備が整ったことになる。

そして、電子銀行サーバＥＢＳは、「電子口座番号」を指定して、その口座番号で示される電子口座が開設された旨を申請局サーバＲＡに通知する（ステップＳＺ７）。

これに応じて、申請局サーバＲＡは、ディレクトリサーバＤＳにアクセスし、そこに予め格納されている「電子銀行署名検証用証明書」、「電子銀行向け暗号用証明書」、「認証局署名検証用証明書」を取得する（ステップＳＺ８）。

ダウンロードする。

（Ｄ２）ＵＩＭ１内で新たに鍵を生成し、認証局サーバＣＡに対しオンラインで公開鍵証明書の発行を依頼する。

ここで、図１３に示すシーケンスを参照しながら、ＵＩＭ１の更新の一例を説明する。以下説明する例では、口座管理料を電子口座から電子バリューを引き落として電子銀行サーバＥＢＳに支払う方式（上記（Ａ１））と、認証局サーバＣＡが生成する新しい鍵対のうち、秘密鍵を移動機ＭＳへダウンロードする方式（上記（Ｃ２））とが選択されている。

電子銀行サーバＥＢＳは、電子口座の継続利用を希望するユーザに対し、事前に口座管理料の引き落とし期日と金額を通知しておく。そして、期日が到来すると、電子銀行サーバＥＢＳは、ユーザの電子口座から、次期分の口座管理料として電子バリューを引き落とす（ステップＳ１）。

次いで、電子銀行サーバＥＢＳは、ユーザの「電子口座番号」に対し、電子署名を施したうえで暗号化して認証局サーバＣＡに通知し、鍵対再発行、ユーザに対する秘密鍵のダウンロード許可、公開鍵証明書発行を依頼する（ステップＳ２）。

一方、認証局サーバＣＡは、復号化と電子署名検証を行い、上記依頼が正しい電子銀行サーバＥＢＳからのものであることを確認したのち、鍵対を生成し、生成した公開鍵の証明書を発行する。発行された公開鍵証明書は、ディレクトリサーバＤＳに登録される（ステップＳ３）。

電子銀行サーバＥＢＳは、ディレクトリサーバＤＳにアクセスして、新しい公開鍵証明書が発行できたことを確認すると（ステップＳ４）、継続利用するユーザの移動機ＭＳに対して、口座管理料を受領したことと秘密鍵のダウンロードに応じる準備が整ったことを通知する（ステップＳ５）。

移動機ＭＳは、電子銀行サーバＥＢＳから秘密鍵のダウンロードに応じる準備が整った通知を受信すると、この通知を表示したのち、ユーザの操作に応じて認証局サーバＣＡに対し新しい秘密鍵のダウンロードを依頼する（ステップＳ６）。

認証局サーバＣＡは、移動機ＭＳからダウンロードの依頼を受け取ると、新し

イムスタンプを付与したうえで、これを要求信号として電子銀行サーバＥＢＳに送信する（ステップＳａ２）。

電子銀行サーバＥＢＳは、上記要求信号を受信すると、受信した電子バリュー情報内の「電子口座番号」を手がかりとして、ディレクトリサーバＤＳから電子署名検証用の公開鍵証明書を取得し、これを用いて移動機ＭＳの電子署名の正当性を検証する（ステップＳａ３）。

次いで、電子銀行サーバＥＢＳは、自身が記憶している「復号用秘密鍵」を用いて、ステップＳａ２で受信した暗号文を復号し、さらにタイムスタンプを確認する（ステップＳａ４）。

このタイムスタンプの確認とは、同一のタイムスタンプが付与された要求信号が同一ユーザから重複して２つ以上受信されたという不都合が起こっていないかどうかを確認する処理である。この処理をすることで、要求信号の不正な再送を防止することができる。

次いで、電子銀行サーバＥＢＳは、指定された引き出し金額あるいは預け入れ金額を確認し、引き出しあるいは預け入れ後における、「ＵＩＭの電子バリュー額」、「電子口座の電子バリュー額」を計算する（ステップＳａ５）。ここでは、引き出し後の「ＵＩＭの電子バリュー額」は１００円となり、「電子口座の電子バリュー額」は９００円となる

次に、電子銀行サーバＥＢＳは、「電子口座番号」を手がかりとしてディレクトリサーバＤＳから暗号用の公開鍵証明書を取得する（ステップＳａ６）。

そして、電子銀行サーバＥＢＳは、ステップＳａ５における計算値のほか、「電子口座番号」、ユーザ名、引き出しまたは預け入れの別を示す取引種別及び取引金額に対し、ディレクトリサーバＤＳから取得した暗号用の公開鍵証明書を用いて暗号化を行う（ステップＳａ７）。

さらに、電子銀行サーバＥＢＳは、上記暗号文に対し、自身が記憶している「署名用秘密鍵」を用いて電子署名を施したうえでタイムスタンプを付与して移動機ＭＳに送信する（ステップＳａ８）。

移動機ＭＳは、受信したデータに対し、電子署名の検証、暗号文の復号、タイ

ュー額を０円から１００円に更新したうえで、この時点のタイムスタンプを発行し、これを「電子バリュー額更新時タイムスタンプ」及び「カレント電子バリュー額更新時タイムスタンプ」として格納する。

そして、電子銀行サーバＥＢＳは、取引が完了した旨のメッセージを移動機ＭＳに送信する（ステップＳａ１６）。

一方、移動機ＭＳは、受信したメッセージを表示し（ステップＳａ１７）、一連の処理は終了する。

上記の例において、ステップＳａ１０におけるキー操作がＮＧの場合は、移動機ＭＳは、ＵＩＭ１内の電子バリュー情報を更新しない。そして、ステップＳａ１２において、ＮＧの旨を示すメッセージを作成し、電子銀行サーバＥＢＳに送信する。

そして、電子銀行サーバＥＢＳは、ＮＧのメッセージを受信すると、ステップＳａ１３において、電子バリュー管理情報を更新せずに処理を終了する。ただし、電子銀行サーバＥＢＳは、上記の処理にかかわるログを移動機ＭＳの電子署名とともに保管しておく。これは、後で当該移動機ＭＳのユーザからの「確認結果としてＯＫを入力したはずだ」というようなクレーム等に対処するために使用する。

さて、例えばステップＳａ１２における移動機ＭＳからのメッセージを電子銀行サーバＥＢＳが受信できない等の理由によって上記処理が完了しない場合は、電子銀行サーバＥＢＳは、取引が完了しなかった旨の不完了メッセージを作成し、そのメッセージと取引前のＵＩＭ１内の電子バリュー額とを、暗号化した上で電子署名を施し、タイムスタンプを付与して移動機ＭＳに送信する。

一方、移動機ＭＳは、不完了メッセージを電子銀行サーバＥＢＳから受信した場合、そのメッセージを表示し、「ＵＩＭの電子バリュー額」を、不完了メッセージと共に送られてきた取引前の「ＵＩＭの電子バリュー額」に置き換える。

また、例えば長期間に渡る通信遮断等により、移動機ＭＳが完了メッセージ又は不完了メッセージのどちらも受信できなかった場合は、移動機ＭＳは、取引未完了の旨を示すメッセージを表示部に表示する。ユーザは、通信遮断等から復旧後、移動機ＭＳを操作して電子銀行サーバＥＢＳに通信接続し、更新後の電子バ

ザＡの電子署名を施して、「ユーザＡが支払う電子バリュー情報」として移動機ＭＳ２に送信する。この際、移動機ＭＳ１は、自身が記憶している電子バリュー情報の中のユーザＡの「電子銀行ＩＤ」、「電子財布種別」、「電子口座番号」及びこれらに対する「電子銀行署名ＳＧＮ１」も合わせて送信する（ステップＳｂ５）。

移動機ＭＳ２は、受信した「電子銀行署名ＳＧＮ１」を検証し、ユーザＡが電子銀行サーバＥＢＳの発行する電子バリューの正当な持ち主であることを確認する（ステップＳｂ６）。確認できない場合は、処理を終了する。

さらに、移動機ＭＳ２は、受信した情報セットに対して施されたユーザＡの電子署名を検証する（ステップＳｂ７）。これにより、第３者がユーザＡの移動機ＭＳ１へなりすますことが防止される。

次いで、移動機ＭＳ２は、受信した「Ａが支払う電子バリュー情報」のうちユーザＡの電子署名を除く情報を表示する（ステップＳｂ８）。即ち、ここでは、ユーザＢの「電子口座番号」、ユーザＡの「電子口座番号」及び「取引金額」１００円が表示されることになる。

ユーザＢは、この表示を参照し、問題がないと判断したら、ＯＫである旨の指示を移動機ＭＳ２に入力する。

一方、ユーザＢが何らかの問題がある判断した場合、ＮＧである旨の指示を移動機ＭＳ２に入力する。移動機ＭＳ２は、ＮＧである旨を移動機ＭＳ１に通知し、処理を終了する。

次に、移動機ＭＳ２は、自身のＵＩＭ１内に記憶されている電子バリュー情報の中の「ＵＩＭのカレント電子バリュー額」に対し、「取引金額」に相当する電子バリュー額１００円を追加し、移動機ＭＳ１から受け取った「Ａが支払う電子バリュー情報」に基づいて「電子バリュー更新履歴」に更新履歴を追加する（ステップＳｂ９）。

次に、移動機ＭＳ２は、「Ａが支払う電子バリュー情報」のうちユーザＡの電子署名を除く情報、即ち、ユーザＢの「電子口座番号」、ユーザＡの「電子口座番号」及び「取引金額」１００円に対してユーザＢの電子署名を施し、これを「Ｂ

なお、電子銀行サーバＥＢＳは、「取引相手電子署名」の検証結果に何らかの問題がある場合は、問題があるため更新できなかった旨のメッセージを作成し、電子銀行サーバＥＢＳの管理者に通知する。

さて、電子銀行サーバＥＢＳは、ステップＳｃ２において更新した電子バリュー管理情報に基づいて、更新すべき電子バリュー情報を移動機ＭＳ２に送信する（ステップＳｃ３）。ここで送信される電子バリュー情報は、「ＵＩＭの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ２」である。

ここで、上記のように「取引相手電子署名」の検証結果に問題がある場合は、上述したような、問題があるため更新できなかった旨のメッセージも合わせて移動機ＭＳ２に送信する。

移動機ＭＳ２は、電子銀行サーバＥＢＳから受信した電子バリュー情報に応じて、自身のＵＩＭ１内の電子バリュー情報を更新する（ステップＳｃ４）。

さて、移動機ＭＳ１は、移動機ＭＳ２と同様に、後に発生した処理において電子銀行サーバＥＢＳと通信する際に、電子銀行サーバＥＢＳから自身の電子バリュー情報のチェックを受ける。

即ち、電子銀行サーバＥＢＳは、移動機ＭＳ１からのアクセスを受けた際に、ユーザＡに対応した「電子バリュー管理情報」のうち、「ＵＩＭのカレント電子バリュー額」と「ＵＩＭの電子バリュー額」を比較する。もし、両者が異なるようであれば電子バリュー管理情報を更新する。ここでの更新内容は、「ＵＩＭの電子バリュー額」を「ＵＩＭのカレント電子バリュー額」に合わせることと、「電子バリュー額更新時タイムスタンプ」を更新することである。

上述した電子バリュー管理情報の更新内容に合わせて、電子銀行サーバＥＢＳは、移動機ＭＳ１に対し、更新すべき電子バリュー情報を送信する。即ち、「ＵＩＭの電子バリュー額」、「電子バリュー額更新時タイムスタンプ」、「電子銀行署名ＳＧＮ２」を送信する。

移動機ＭＳ１は、電子銀行サーバＥＢＳから受信した電子バリュー情報のうち、「電子銀行署名ＳＧＮ２」を検証し、問題がなければ、ＵＩＭ１内の電子バリュ

電子銀行サーバ向け暗号用公開鍵による暗号化を行い、「署名用秘密鍵」を用いて電子署名を施したデータを、振込みを要求する要求信号として電子銀行サーバＥＢＳに送信する（ステップＳｄ２）。

なお、ステップＳｄ１において、ユーザがプリペイドカードＰＣを振り込み元として選択した場合は、移動機ＭＳはプリペイドカードＰＣと赤外線通信を行ってプリペイドカードＰＣ内の電子バリュー情報を取得し、これも同時に電子銀行サーバＥＢＳに送信する。

一方、電子銀行サーバＥＢＳでは、受信したデータに対し、電子署名の検証を行い、暗号文の復号化を行い、タイムスタンプを確認することによって、電子バリュー情報の正当性を確かめる（ステップＳｄ３）。

次に、電子銀行サーバＥＢＳは、指定された振り込み先電子口座が入金可能あるいは開設状態で実在すること、及び振り込み元の電子バリューの残高が指定された振込金額以上であることを確認する（ステップＳｄ４）。

なお、プリペイドカードＰＣが振り込み元として選択されている場合、電子銀行サーバＥＢＳは、「電子銀行署名ＳＧＮ４」を検証し、振り込み元（プリペイドカードＰＣ）の電子バリュー情報が不正に書き換えられていないことを確認した上で振り込み可能かを確認する。

次に、電子銀行サーバＥＢＳは、振り込み後の振り込み元（ここではＵＩＭ１）の電子バリュー額を計算する。そして、「電子銀行ＩＤ」、振り込み先電子口座番号、振り込み先電子口座のユーザ名、振り込み金額、振り込み元のユーザの「電子口座番号」、振り込み前後の振り込み元（ＵＩＭ１）の電子バリュー額に対し、タイムスタンプを付与し、ディレクトリサーバＤＳから取得した暗号用公開鍵による暗号化を行い、自身が記憶する「署名用秘密鍵」を用いて電子署名を施して移動機ＭＳに送信する（ステップＳｄ５）。

移動機ＭＳは、受信したデータの電子署名を検証し、暗号文を復号し、タイムスタンプを確認することにより、不正がないことを確かめる（ステップＳｄ６）。

次いで、移動機ＭＳは、受信したデータを表示する。ユーザがこれを目視確認し、ＯＫあるいはＮＧを示す入力操作を行うと、移動機ＭＳはこれを受け付ける

さて、例えばステップＳｄ８において、移動機ＭＳからのメッセージを電子銀行サーバＥＢＳが受信できない等の理由により上記処理が完了しない場合は、電子銀行サーバＥＢＳは、移動機ＭＳに対し、取引が完了しなかった旨の不完了メッセージ、及び取引前の「ＵＩＭの電子バリュー額」を、ステップＳａ８と同様に、暗号化した上で電子署名を施し、タイムスタンプを付与して移動機ＭＳに送信する。

一方、移動機ＭＳは、不完了メッセージを電子銀行サーバＥＢＳから受信した場合、そのメッセージを表示し、「ＵＩＭの電子バリュー額」を、不完了メッセージと共に送られてきた取引前の「ＵＩＭの電子バリュー額」に置き換える。

また、例えば長期間に渡る通信遮断等により、移動機ＭＳが完了メッセージ又は不完了メッセージのどちらも受信できなかった場合は、移動機ＭＳは、取引未完了の旨を示すメッセージを表示部に表示する。ユーザは、通信遮断等から復旧後、移動機ＭＳを操作して電子銀行サーバＥＢＳに通信接続し、更新後の電子バリュー情報を取得して自身の電子バリュー情報を更新する。

上記の例においては、移動機ＭＳのＵＩＭ１内の電子バリューを例にあげて説明したが、プリペイドカードＰＣ内の電子バリューから振り込む場合には、プリペイドカードＰＣは赤外線通信を行うことにより移動機ＭＳを介して上記と同様の処理を行えばよい。

Ｃ：応用例

次に、実施形態の応用例について説明する。

例えば自動販売機やＰＯＳ（Point Of Sale）レジに対し、移動機ＭＳのＵＩＭ１に相当する電子財布の機能を組み込み、顧客（即ち自動販売機等の利用者）の移動機ＭＳ（若しくはプリペイドカードＰＣ）と自動販売機との間で、ローカルな通信により電子財布間の電子バリュー受け渡しを行ない、キャッシュレスで商品を販売することができる。

自動販売機においては、移動機ＭＳと電子バリューをやり取りする時点で「電子銀行署名ＳＧＮ１」を検証することにより、その正当性を確認することができるため、その都度電子銀行サーバＥＢＳに当該電子バリュー情報の正当性を確認

電子バリュー額に相当する金額情報が商品金額以上であることを確認する。これが不足している場合は、自動販売機ＶＭは、当該移動機ＭＳにかかわる処理を中止し、金額不足の旨のメッセージを移動機ＭＳに返信する。

自動販売機ＶＭは、上記の金額を確認したら、受信した、自動販売機業者の「電子口座番号」、顧客の「電子口座番号」、支払う電子バリュー額及び顧客の電子署名を「電子バリュー更新履歴」としてログをとる。

そして、自動販売機ＶＭは、商品代金を受領した旨のメッセージを作成し、それに電子署名を施して移動機ＭＳに返信する。この時点で、顧客の自動販売機ＶＭへの商品代金の支払いは完了し、顧客は自動販売機ＶＭの商品選択のボタンを押し下げることができるようになり、顧客がボタンを押し下げて、商品の受け渡しが完了する。

そして、移動機ＭＳは、自動販売機ＶＭから受信したメッセージに基づいて、ＵＩＭ１内の電子バリュー情報を更新する。具体的には、「カレント電子バリュー額」から支払った商品の代金を引き、「電子バリュー更新履歴」に、自動販売機業者の「電子口座番号」、顧客の「電子口座番号」、支払う電子バリュー額及び自動販売機ＶＭの電子署名を追加する。

自動販売機ＶＭに蓄積されたログは、定期的に自販機サーバＶＳによって収集され、電子銀行サーバＥＢＳへ送られる。

電子銀行サーバＥＢＳサーバでは、自販機サーバＶＳから受け取った「電子バリュー更新履歴」に対して、支払い者の電子署名を検証し、以下の管理情報を変更する。

即ち、自動販売機ＶＭ業者の電子口座の電子バリュー管理情報については、「電子口座の電子バリュー額」を追加し、電子口座の「電子バリュー額更新時タイムスタンプ」更新する。顧客の電子口座・電子財布の電子バリュー管理情報については、ＵＩＭ１の「カレント電子バリュー額」減額、「電子バリュー額更新時タイムスタンプ」更新する。

ここで、顧客がプリペイドカードＰＣで支払った場合においては、プリペイドカードＰＣについて、「プリペイドカードのカレント電子バリュー額」減らし、

また、電子銀行サーバＥＢＳは、少なくともいずれか一方の電子財布からの通知により、自身が管理している電子バリュー管理情報を更新するので、効率性が向上する。

また、取引時にはタイムスタンプを付与するので、これを検証することで不正な再送信を防止することができる。

Ｄ：変形例

既述の通り、本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

（１）移動機ＭＳの形態

移動機ＭＳは、無線通信機能を内蔵する携帯端末であればよく、上述した携帯電話機のほかにも、携帯電話機に接続してデータ通信を行なうパーソナルコンピュータまたはＰＤＡ（Personal Digital Assistants）等であってもよい。

（２）移動機、プリペイドカード、自動販売機の通信形態

実施形態では、移動機ＭＳ、プリペイドカードＰＣ、自動販売機ＶＳは互いに赤外線を用いた無線通信を行うようになっていたが、これに限らず、有線通信であってもよい、

例えば、移動局５０は、シリアル信号の入出力を行う１６芯コネクタを一般に備えているが、これと同様のものをプリペイドカードＰＣや自動販売機ＶＳ側にも備え、これらコネクタを介して、相互にケーブル接続することによりデータ通信を行うようにしてもよい。

（３）各サーバの設置形態

前記実施形態においては、電子銀行サーバＥＢＳは移動通信網ＭＮ上に設置され、申請局サーバＲＡ、認証局サーバＣＡ及びディレクトリサーバＤＳは、インターネットＩＮＥＴ上の設置されていた。しかし、これに限らず、各サーバはどのようなネットワーク上にあってもよい。

（４）鍵対の生成

実施形態では、申請局サーバＲＡがユーザの鍵対を生成し、ＵＩＭ１に書き込むようにしていたが、これに限らない。

電子銀行サーバＥＢＳに送信するようにしてもよい。これにより、電子財布側の電子バリュー情報と電子銀行側の電子バリュー情報とを整合させる。

また、移動機ＭＳは、電子財布の記憶容量に相当する量「電子バリュー更新履歴」を蓄積したことを検出すると、それ以後、電子バリューを利用した取引を行わないようにしてもよい。その場合、移動機ＭＳは、その旨を表示部に表示させてユーザに通知する等の処理を行う。

（６）移動機ＭＳ及びプリペイドカードＰＣ間の通信手段

移動機ＭＳ及びプリペイドカードＰＣ間のローカルな通信手段は、上述した赤外線通信に限定されるわけではなく、これとは異なる無線通信手段、例えばブルートゥース（登録商標）であってもよい。もちろん、移動機ＭＳ及び自動販売機ＶＭ間の通信手段についても、同様に、赤外線以外の無線通信手段を用いることも可能である。

取引ログとして送信し、

前記財布残金管理手段は、前記送信されてくる取引ログに基づいて、前記電子バリューの残高情報を更新することを特徴とする電子バリューシステム。

3．請求項2に記載の電子バリューシステムにおいて、

前記第1の通信端末及び前記第2の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、

前記第1の通信端末又は前記第2の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する量の前記取引ログを蓄積すると、外部ノードと電子バリューの送受信を行わないことを特徴とする電子バリューシステム。

4．請求項2に記載の電子バリューシステムにおいて、

前記第1の通信端末及び前記第2の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、

前記第1の通信端末又は前記第2の通信端末のうち少なくともいずれか一方は、前記ログ蓄積手段による記憶容量に相当する量の前記取引ログを蓄積すると、それ以後の取引時においては取引日時の古い順から前記取引ログを消去することを特徴とする電子バリューシステム。

5．請求項2に記載の電子バリューシステムにおいて、

前記第1の通信端末及び前記第2の通信端末は、自身の取引にかかる前記取引ログを蓄積するログ蓄積手段を有し、

前記取引ログ通知手段は、前記第1の通信端末又は前記第2の通信端末のうち少なくともいずれか一方において前記ログ蓄積手段による記憶容量に相当する量の前記取引ログを蓄積すると、当該取引ログを前記財布残金管理手段に送信することを特徴とする電子バリューシステム。

バリューを送受信する電子バリューシステムであって、

前記第１の通信端末は、

前記電子バリューと、前記電子バリューを発行した発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納するメモリと、

前記発行主体の識別情報及び電子署名を、前記格納されている電子バリューとともに、前記第２の通信端末に送信するための送信手段とを備え、

前記第２の通信端末は、

前記第１の通信端末から送信された電子バリューとともに、前記発行主体の識別情報及び電子署名とを受信する受信手段と、

前記受信した電子署名を検証することにより、前記第１の通信端末から送信された電子バリューが前記発行主体により発行されたことを確認することによって前記第１の通信端末の正当性を判断する判断手段と

を備えることを特徴とした電子バリューシステム。

１２．請求項１１に記載の電子バリューシステムであって、

前記第２の通信端末は、

前記電子バリューと、当該電子バリューを発行した発行主体の識別情報と、当該識別情報に対し前記発行主体によって施された電子署名とを格納するメモリと、

前記格納されている前記発行主体の識別情報及び電子署名を前記第１の通信端末に送信するための送信手段とをさらに備え

前記第１の通信端末は、

前記第２の通信端末に対し前記電子バリューを送信する前に、前記第２の通信端末のメモリ内の前記発行主体の識別情報と当該識別情報に対し前記発行主体によって施された電子署名を取得する取得手段と、

前記取得した電子署名を検証し、前記第２の通信端末のメモリ内の電子バリューは前記発行主体により発行されたことを確認することによって、前記第２の通信端末の正当性を判断する判断手段とをさらに備えることを特徴とした電子バリューシステム。

外部と前記電子バリューを送受信する際に、当該電子バリューに対し鍵を用いて電子認証及び暗号・復号の処理を行うセキュリティ手段と、

前記鍵を定期的に更新する更新手段と

を備えることを特徴とする電子バリューシステム。

１９．電子的な金銭情報である電子バリュー及び自己の識別情報を格納するメモリと、

外部ノードとの間で前記電子バリューの送受信を行う通信手段と、

前記メモリに格納されている自己の識別情報を前記外部ノードに与える一方、前記外部ノードから当該外部ノードの識別情報を取得する識別情報交換手段と、

前記外部ノードとの間で送受信された前記電子バリューの額と、前記自己の識別情報及び前記外部ノードの識別情報とを取引ログとして蓄積するログ蓄積手段と

を備えることを特徴とする通信端末。

２０．請求項１９に記載の通信端末において、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、前記外部ノードとの間で前記電子バリューの送受信を行わないことを特徴とする通信端末。

２１．請求項２０において、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、それ以後の前記電子バリューの送受信時においては、前記蓄積されている取引ログを送受信日時の古い順から消去することを特徴とする通信端末。

２２．請求項２１において、前記ログ蓄積手段による記憶容量に相当する前記取引ログを蓄積すると、前記蓄積されている取引ログを、当該取引ログを用いて前記電子バリューの送受信についての正当性を確認する外部装置に送信することを特徴とする通信端末。

を備えることを特徴とする通信端末。

２８．請求項２７に記載の通信端末において、

前記通信端末は、外部と前記電子バリューを送受信する際に、当該電子バリューに対し鍵を用いて電子認証及び暗号・復号の処理を行うセキュリティ手段と、

前記鍵を定期的に更新する更新手段と

を備えることを特徴とする通信端末。

２９．請求項２７に記載の通信端末において、

前記電子バリューを前記外部ノードに送信する際に、その送信日時を前記電子バリューに付加して送信することを特徴とする通信端末。

３０．請求項２７に記載の通信端末において、

前記通信手段は、無線により前記外部ノードとの間で前記電子バリューの送受信を行うことを特徴とする通信端末。

３１．請求項２７に記載の通信端末において、

前記通信端末は、移動通信網に収容される移動通信端末であり、

前記メモリは、当該通信端末に装着して使用されるＩＣカードであることを特徴とする通信端末。

３２．電子的な金銭情報である電子バリューを記憶するサーバであって、ユーザに割り当てられた電子口座毎に前記電子バリューを蓄積する電子口座保持手段と、前記電子バリューを格納するメモリと、外部ノードとの間で前記電子バリューを送受信する通信手段とを有した通信端末に対し、前記電子口座保持手段によって蓄積されている電子バリューを前記ネットワークを介して移す移行手段と、

前記通信端末のメモリに格納される電子バリューの残高情報を記憶する財布残金記憶手段とを備え、

図 1

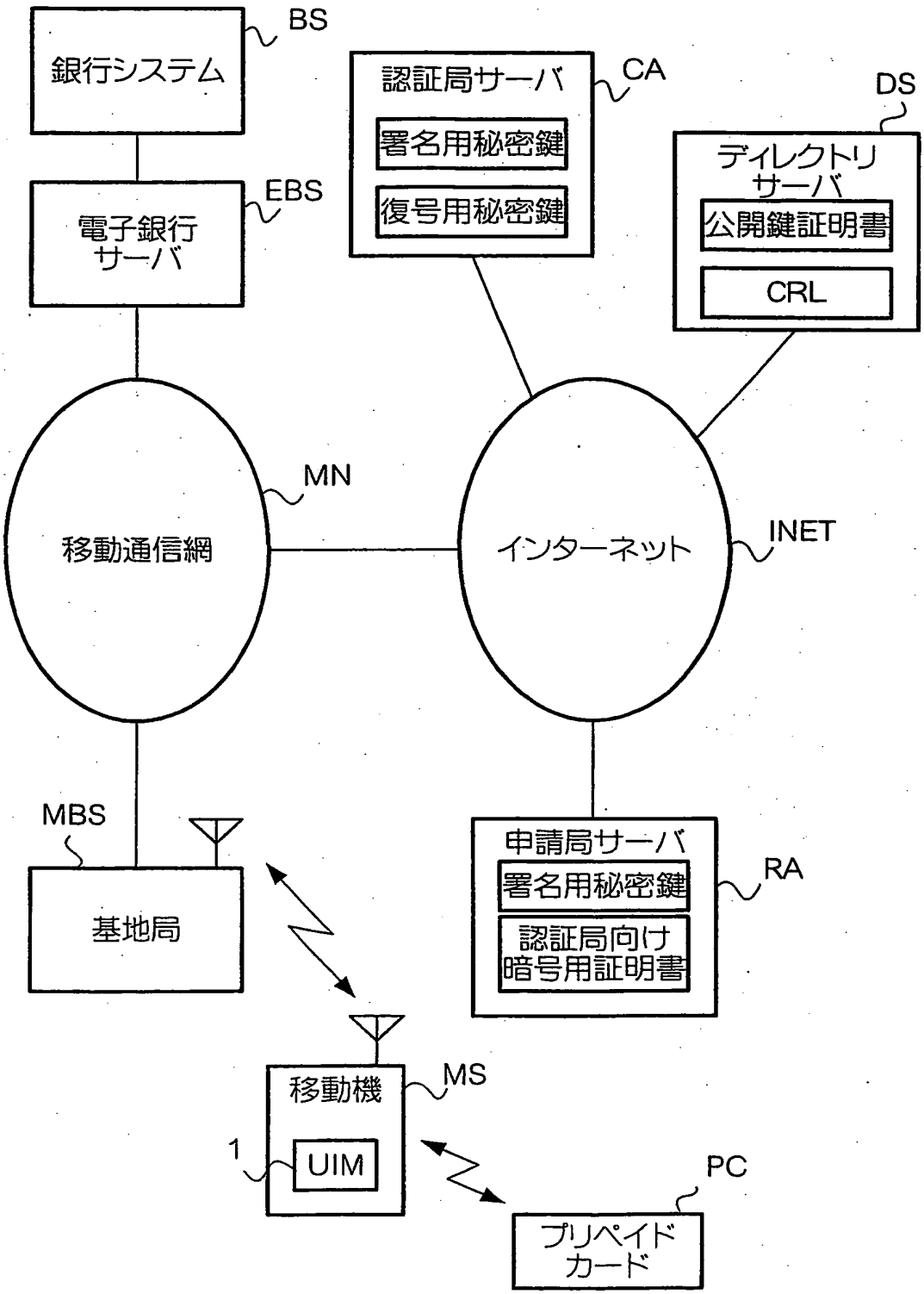

銀行システム
BS
電子銀行
サーバ
EBS
認証局サーバ
CA
署名用秘密鍵
復号用秘密鍵
DS
ディレクトリ
サーバ
公開鍵証明書
CRL
移動通信網
MN
インターネット
INET
MBS
基地局
申請局サーバ
署名用秘密鍵
認証局向け
暗号用証明書
RA
移動機
MS
1
UIM
PC
プリペイド
カード

図 4

通番	データ名	説明
1	電子銀行 ID	電子バリューを発行した電子銀行サーバ EBS を識別するための識別情報
2	電子口座番号	電子口座の識別情報
3	電子口座の電子バリュー額	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点の電子口座の電子バリューの残高
4	UIM の電子バリュー額	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点における、UIM1 に格納されている電子バリューの残高
5	電子バリュー額更新時タイムスタンプ	上記通番 4 の電子バリュー額が電子銀行サーバ EBS によって更新された時点で付与される日時情報
6	電子口座のカレント電子バリュー額	電子口座内の最新の電子バリューの残高
7	UIM のカレント電子バリュー額	UIM1 に反映すべき電子バリューの残高
8	カレント電子バリュー額更新時タイムスタンプ	上記通番 6 及び 7 の電子バリュー額を電子銀行サーバ EBS が更新した時点で電子銀行サーバ EBS が付与する日時情報
9	電子バリュー更新履歴	移動機 MS が最後に電子銀行サーバ EBS とアクセスした時点から現在までの UIM の電子バリュー額の更新履歴

図 6

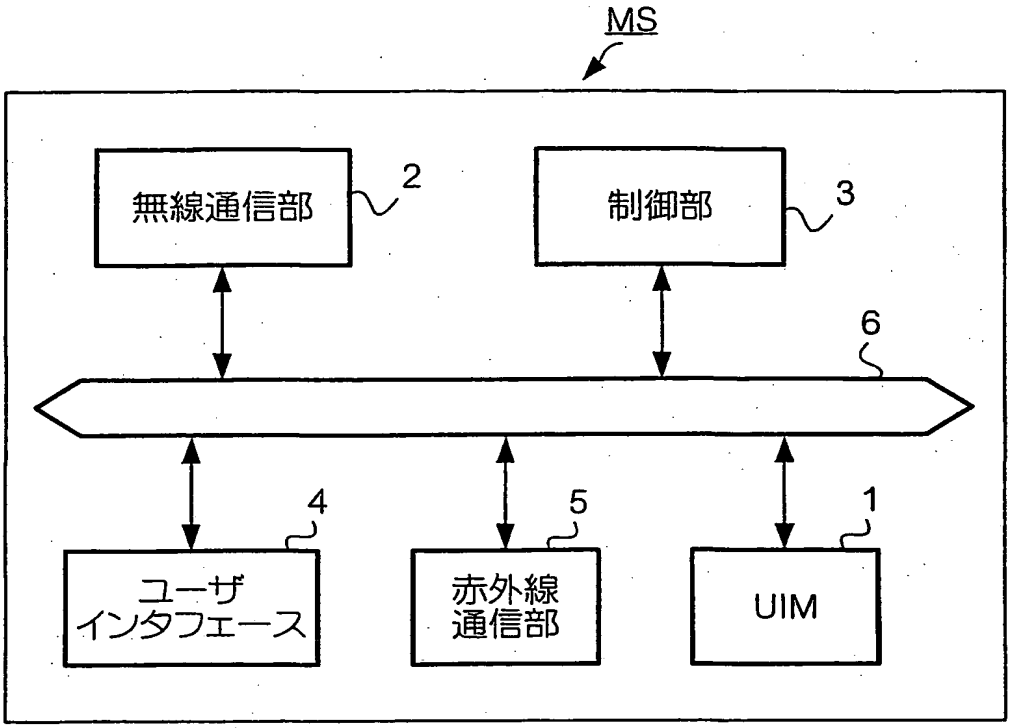


図 7

通番	データ名	説明
1	署名用秘密鍵	移動機 MS が送信するﾃﾞｰﾀに対し、電子署名を施すための秘密鍵
2	復号用秘密鍵	移動機 MS が受信した暗号文を復号するための秘密鍵
3	電子銀行署名検証用証明書	電子銀行ｻｰﾊﾞ EBS によって施された電子署名を検証するための公開鍵の証明書
4	電子銀行向け暗号用証明書	電子銀行ｻｰﾊﾞ EBS へ送信するﾃﾞｰﾀを暗号化するための公開鍵の証明書
5	認証局署名検証用証明書	認証局 CA によって各種証明書上に施された電子署名を検証するための公開鍵の証明書
6	ﾕｰｻﾞ ID	移動機ﾕｰｻﾞの識別情報
7	電子ﾊﾞﾘｭｰ情報	UIM1 及び電子口座内の電子ﾊﾞﾘｭｰに関する情報

図 9

通番	データ名	説明
1	受取側電子口座番号	電子バリューを受け取る側の電子口座番号
2	支払側電子口座番号	電子バリューを支払う側の電子口座番号
3	支払側プリペイドカードID	電子バリューの支払がプリペイドカードの場合における、プリペイドカードID
4	取引金額	電子バリューの受取側と支払側とで取引された金額
5	取引相手電子署名	取引相手の電子署名

図 10

通番	データ名	説明
1	電子銀行署名検証用証明書	電子銀行サーバEBSによって施された電子署名を検証するための公開鍵の証明書
2	電子銀行向け暗号用証明書	電子銀行サーバEBSへ送信するデータを暗号化するための公開鍵の証明書
3	認証局署名検証用証明書	認証局CAによって各種証明書上に施された電子署名を検証するための公開鍵の証明書
4	電子バリュー情報	プリペイドカードPC内の電子バリューに関する情報

図 12

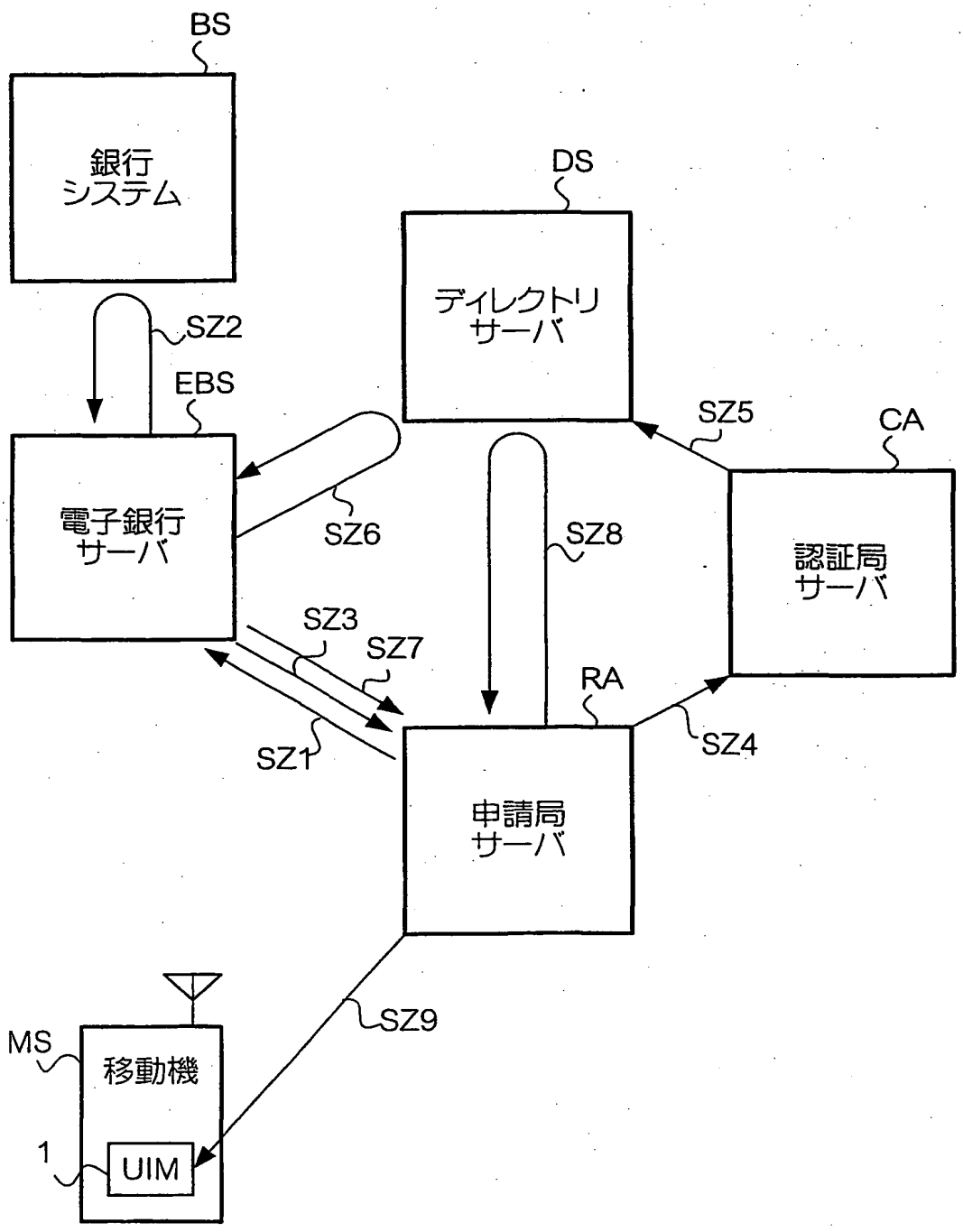

BS
銀行
システム
DS
ディレクトリ
サーバ
SZ2
EBS
SZ5
CA
電子銀行
サーバ
SZ6
SZ8
認証局
サーバ
SZ3
SZ7
RA
SZ1
SZ4
申請局
サーバ
SZ9
MS
移動機
1
UIM

図 14

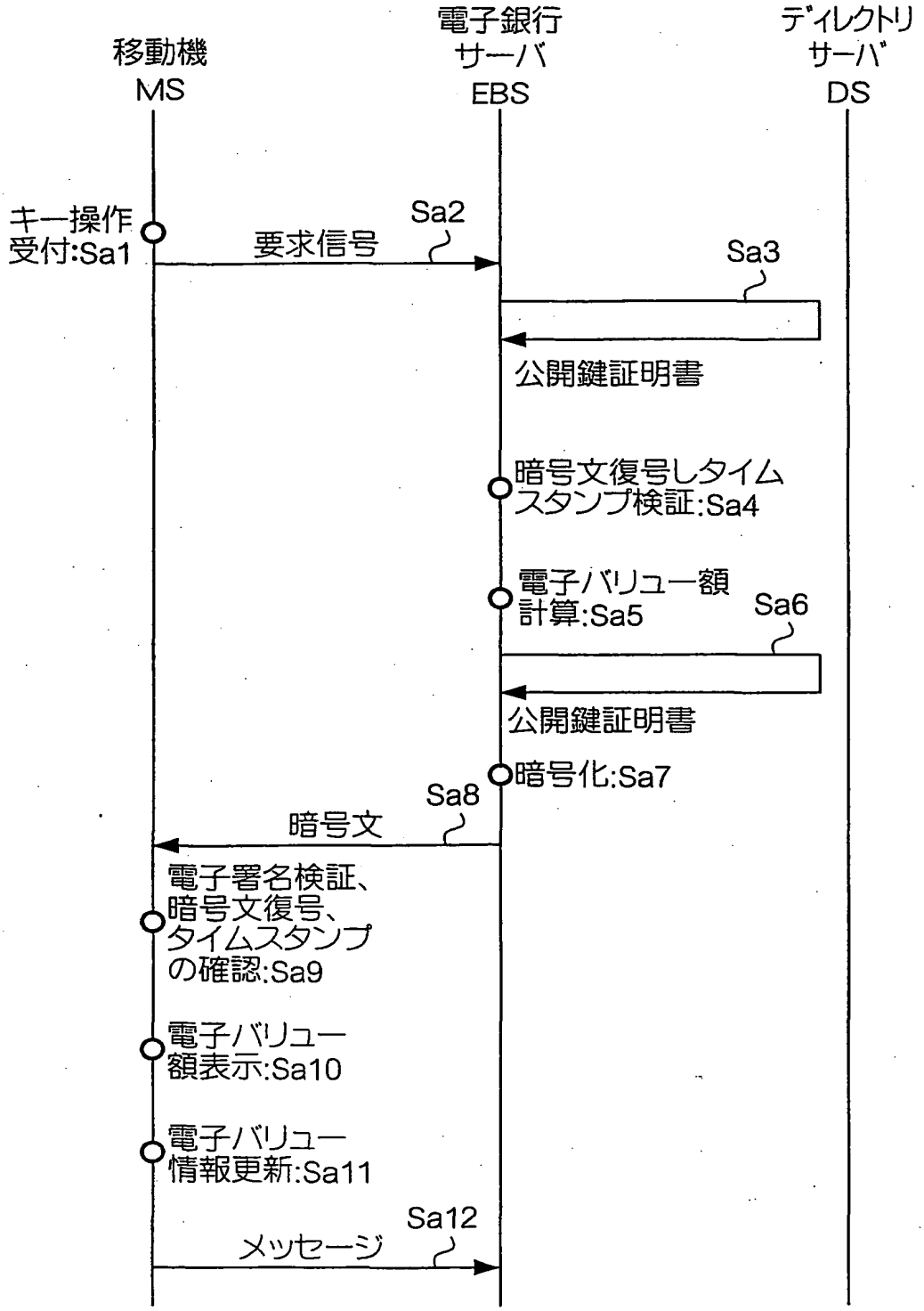

移動機
MS
電子銀行
サーバ
EBS
ディレクトリ
サーバ
DS
キー操作
受付:Sa1
要求信号
Sa2
Sa3
公開鍵証明書
暗号文復号しタイム
スタンプ検証:Sa4
電子バリュー額
計算:Sa5
Sa6
公開鍵証明書
暗号化:Sa7
Sa8
暗号文
電子署名検証、
暗号文復号、
タイムスタンプ
の確認:Sa9
電子バリュー
額表示:Sa10
電子バリュー
情報更新:Sa11
Sa12
メッセージ

図 16

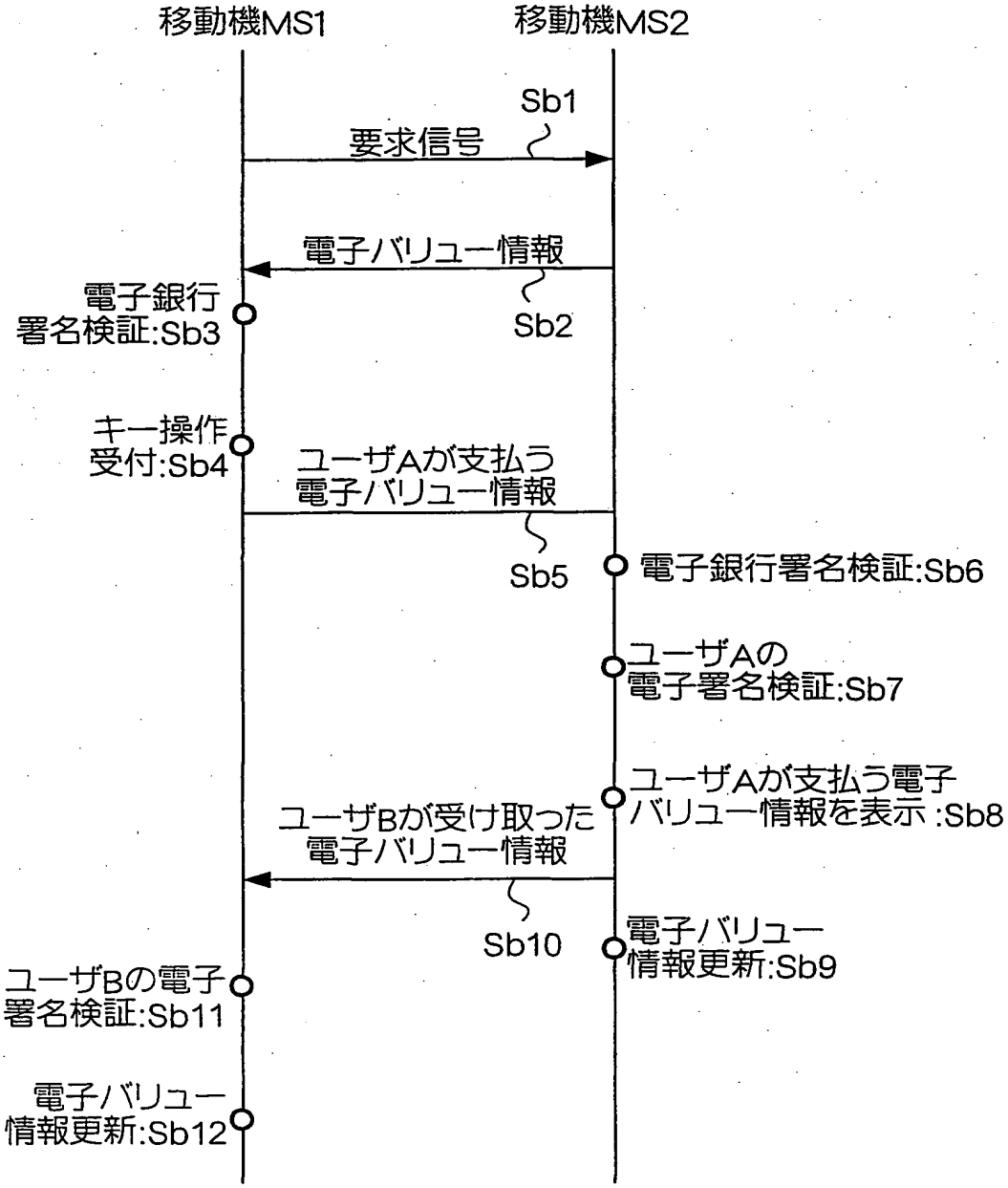
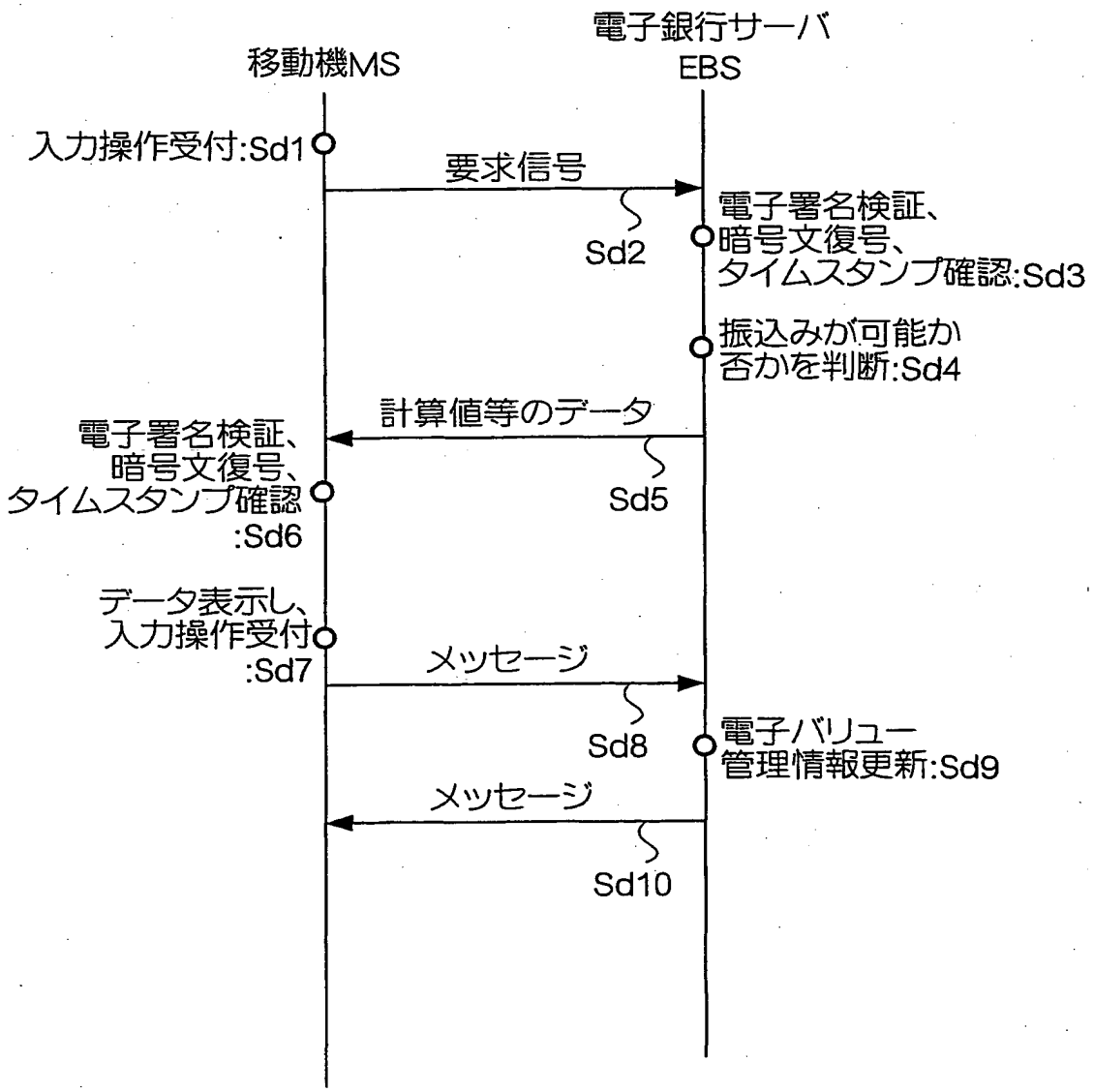

移動機MS1
移動機MS2
Sb1
要求信号
電子バリュー情報
電子銀行
署名検証:Sb3
Sb2
キー操作
受付:Sb4
ユーザAが支払う
電子バリュー情報
Sb5
電子銀行署名検証:Sb6
ユーザAの
電子署名検証:Sb7
ユーザAが支払う電子
バリュー情報を表示 :Sb8
ユーザBが受け取った
電子バリュー情報
Sb10
電子バリュー
情報更新:Sb9
ユーザBの電子
署名検証:Sb11
電子バリュー
情報更新:Sb12

図 18


電子銀行サーバ
EBS
移動機MS
入力操作受付:Sd1
要求信号
Sd2
電子署名検証、
暗号文復号、
タイムスタンプ確認:Sd3
振込みが可能か
否かを判断:Sd4
計算値等のデータ
Sd5
電子署名検証、
暗号文復号、
タイムスタンプ確認
:Sd6
データ表示し、
入力操作受付
:Sd7
メッセージ
Sd8
電子バリュー
管理情報更新:Sd9
メッセージ
Sd10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/04538

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 99/24892 A1 (Citicorp Development Center Inc.), 20 May, 1999 (20.05.99), page 11, lines 27 to 29 & AU 92346/98 A & EP 917120 A2 & JP 11-232348 A & SG 78323 A	1-33
Y	WO 93/08545 A1 (Jonhig Ltd.), 29 April, 1993 (29.04.93), Figs. 3 to 5 & AU 28886/92 A & AU 663739 B & BR 9205416 A & CA 2098481 A & DE 69215501 D & EP 567610 A1, B1 & ES 2096772 T & GR 3022528 T & HK 1001573 A & JP 6-503913 A & JP 2853331 B2 & KR 161670 A & MD 1402 F & NO 303893 B & PL 299825 A & RU 2137187 A & US 5440634 A	1-33

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 August, 2001 (28.08.01)	11 September, 2001 (11.09.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０１／０４５３８

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F17／60

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F17／60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2001年
日本国登録実用新案公報　1994－2001年
日本国実用新案登録公報　1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 99/24892 A1 (CITICORP DEVELOPMENT CENTER INC) 20. 5月. 1999 (20.05.99) *11 ページ, 27–29 行* & AU 92346/98 A　& EP 917120 A2 & JP 11-232348 A　& SG 78323 A	1–33

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
28.08.01	11.09.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	阿波　進　印	５Ｌ　９１６８
	電話番号　０３－３５８１－１１０１　内線　３５６１	

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）